

We are IntechOpen, the world's leading publisher of Open Access books Built by scientists, for scientists

4,800

Open access books available

122,000

International authors and editors

135M

Downloads

Our authors are among the

154

Countries delivered to

TOP 1%

most cited scientists

12.2%

Contributors from top 500 universities



WEB OF SCIENCE™

Selection of our books indexed in the Book Citation Index
in Web of Science™ Core Collection (BKCI)

Interested in publishing with us?
Contact book.department@intechopen.com

Numbers displayed above are based on latest data collected.
For more information visit www.intechopen.com



Attacks on the HF Physical Layer of Contactless and RFID Systems

Pierre-Henri Thevenon¹, Olivier Savry¹,
Smail Tedjini² and Ricardo Malherbi-Martins¹

¹*Leti, MINATEC, CEA Grenoble*

²*LCIS Lab, Grenoble-INP Valence
France*

1. Introduction

During the past few years, RFID technology has strongly penetrated in our lives. Nowadays public transportation ticketing, passports, ID cards, driving licenses and credit cards are using the electromagnetic waves to improve the quickness of the exchanged data. RFID devices can be divided in two main classes: the contactless cards which are smartcards with a wireless inductive interface compliant to the ISO14443 or ISO15693 standards, and the RFID tags which can have an HF or UHF interface compliant to the ISO18000 standard which now includes the EPCGlobal contribution. RFID tags are mainly dedicated to identification of objects. These exhibit a large reading distance but provide poor computational and processing resources. RFID devices and smartcards have a common characteristic; their contactless interface adds threats in term of security and privacy. This chapter will deal with this specificity by moving apart the well-known physical threats on smartcards like side channel attacks. Indeed, it is worth pointing out that the RF channel opens new potential vulnerabilities which could jeopardize security and as a consequence they should be listed and studied:

- Bidirectional data communication over the air:
The transactions can be easily eavesdropped by a spying probe within a distance of several meters. Due to the low resources feature of such a device, encryption remains difficult to implement.
- Unidirectional power transfer over the air:
The device is not the master of its energy which should be provided by the reader or by the attacker opening a backdoor for denial of service.
- Clock transfer over the air (especially for HF interface):
The sequencer of the card can be monitored by the reader or the attacker. Pauses or accelerations of the processor can be achieved.
- Passive devices and no ON/OFF switch:
The owner of the card or the tag is not able to switch off his device involving a main threat for its privacy.
- Load based retro-modulation:

The communication from the tag to the reader is really weak and performed in a passive way without emission of electromagnetic field but with modulation of the load at the terminals of the tag antenna. It can be easily blurred or modified.

- Singulation or Anti-collision protocol:
The reader should have to deal with numerous tags or cards in its field. It requires a kind of identification which could endanger privacy.

This chapter proposes an overview of all these physical layer attacks.

2. Security & privacy

The vulnerabilities introduced by the contactless standards should be seen as vectors for attacks and as causes for risks on the security of the system and on privacy of people. Those two latter issues could be considered as antagonists. On the one hand, companies which deploy or use RFID systems naturally target profits and as a consequence try to nullified fraud which could be a severe competitor, to protect their business. On the other hand, for privacy, the point of view has changed: the security is no longer seen from the eyes of the provider but with the eyes of the user. More and more, users will live in a digital world with one or several digital doubles. So, the issue becomes individual freedom and more specifically in this case the protection of personal data and the insurance of not being spied or traced. Tracking a person by scanning tags or cards on him, using the access card without the agreement of its owner to enter in a secure building, all these attacks can be currently done by using information in contactless cards or RFID tags memory. For these reasons, contactless technology is often associated with privacy invasions, population under surveillance. The interests of the user and of the provider could be shared if the latter realizes that privacy is framed by regulatory matters sometimes dedicated to RFID like European recommendations and that it is a condition of a large scale deployment of RFID. Risk analysis should be performed on these two main topics: prevention of economical fraud and preservation of privacy. The targeted assets and the motivation of attackers differ even if countermeasures could help both. Vulnerabilities and attacks to security or privacy lead mainly to four risks:

- Eavesdropping on the communication:
In the field of privacy, identifier of tags could be listened enabling tracking or impersonation of tags. For the security of the system, secret data like session keys could leak.
- Remote activation without the consent of the owner:
This is the main threat to privacy since silent physical tracking and inventorying of people possessions could be carried out. This risk is also the basis of the relay attack which is able to circumvent any cryptographic protocol.
- Denial of service: the system becomes inoperative:
Due to the weak signal answered by the tags, it is easy to blur it. The simple destruction of the tag is also possible by applying an over estimated field. Many solutions exist that could lead to an out of order system.
- Unique identifier which is a pointer on a database:
The fact that each items bought in a supermarket will be tagged with an unique identifier will enable to trace it and to fill all the properties of the object and of the owner in a database.

All those risks require to study in detail the attacks which are at their origin.

3. Eavesdropping

Eavesdropping is a passive attack, which consists in secretly listening a private communication between a reader and a card (Figure 1). This attack, particularly simple to realize, is a true threat because the attacker can analyze transmitted data between the reader and the card to recover confidential information.



Fig. 1. Eavesdropping attack

3.1 State of art

First experiments on eavesdropping attacks were published by the NIST (National Institute of Standard and Technology) in 2004. Researchers have succeeded in recovering e-passport private data situated at 9 metres from their spy. Despite the lack of details in the description of the measurement protocol, it seems that only the forward communication (communication from the reader to the card) has been eavesdropped (Hoshida, 2004). Furthermore, it seems that ISO14443-B standard is more sensitive to eavesdropping attacks than devices using ISO14443-A (ISO/IEC14443-2, 2001).

In 2004, Finke and Kelter of BSI (German federal office for information security) have presented results demonstrating that a communication between an NXP contactless reader and a card can be intercepted at 2 metres (Finke & Kelter, 2004). The main feature of their attack is the use of a specific position of the spy antenna called second Gauss position (see part 3.2).

A report from the FOIS (Federal Office for Information Security) has described all threats specific to the contactless link. No experience is described in this paper, but the main features of the attack are given. Anti-collision protocols amplify the risk factor because confidential data are repeated during theses protocols. Based on theoretical studies, it seems that an attacker may listen the uplink communication up to few dozens of metres and only 50 cm for the downlink communication (FOIS, 2004).

In 2006, researchers of the NIST have realized experiments using an NXP reader, compliant to the ISO14443-A standard (Guerrieri & Novotny, 2006). Their work shows the influence of the spy antenna positions; two position, called Gauss, positions are described. They succeed in spying a communication up to 6.5 metres in the first position and up to 15 metres in the second position. The characteristics of these positions will be explained in the section 3.2.

Hancke has presented experiments on the main attacks that occurred on the physical layer. His paper gives a lot of information on the measurement protocol, particularly on the used equipment (Hancke, 2006). The results show that the entire communication (forward and backward) can be eavesdropped at a distance of 4 metres. The author has completed this

first article with a new paper by adding new results and conclusions in 2008. The measurement protocol is well detailed and all HF standards are studied. During these experiments, the results are sampled then processed on a computer in order to enlarge the spying distance. It shows that forward communication is easier to recover than the downlink communication (Hancke, 2008a, 2008b).

3.2 Theoretical study on Gauss positions

The position of the attacker antenna with respect to the reader antenna has an important influence on the amplitude of the signal recovered by the spy antenna. Two positions are particularly important; they are called Gauss positions and are used in few attacks described in the state of art (previous section). To enlarge the eavesdropping distance of an attacker, a theoretical study will be made on the Gauss position. A loop antenna can be considered as a magnetic dipole antenna when the diameter of the emission antenna is much smaller than the distance between the antenna and the observation point (Figure 2a).

Equations 1, 2 and 3 give magnetic and electric fields seen as a distance r of the emission loop antenna.

$$H_{\theta} = \frac{I.S.\sin\theta}{4\pi r^3} \left(1 + j\frac{2\pi r}{\lambda} - \frac{4\pi^2 r^2}{\lambda^2}\right) e^{j(\omega t - 2\pi r/\lambda)} \quad (1)$$

$$H_r = \frac{I.S.\cos\theta}{2\pi r^3} \left(1 + j\frac{2\pi r}{\lambda}\right) e^{j(\omega t - 2\pi r/\lambda)} \quad (2)$$

$$E_{\phi} = j\pi \frac{I.S.\sin\theta}{\omega\epsilon_0\lambda^2 r^2} \left(1 + j\frac{2\pi r}{\lambda}\right) e^{j(\omega t - 2\pi r/\lambda)} \quad (3)$$

Equations are used to predict the magnetic field in the case of the two Gauss positions, i.e. with $\theta = 0^\circ$ for the first position and $\theta = 90^\circ$ for the second position. The results on Figure 2b show that the first gauss position is more interesting when the attacker is situated at a distance smaller than 8 metres. When distance is larger than 8 metres, the second Gauss position will allow an attacker to obtain the highest RF field amplitude on the spying antenna.

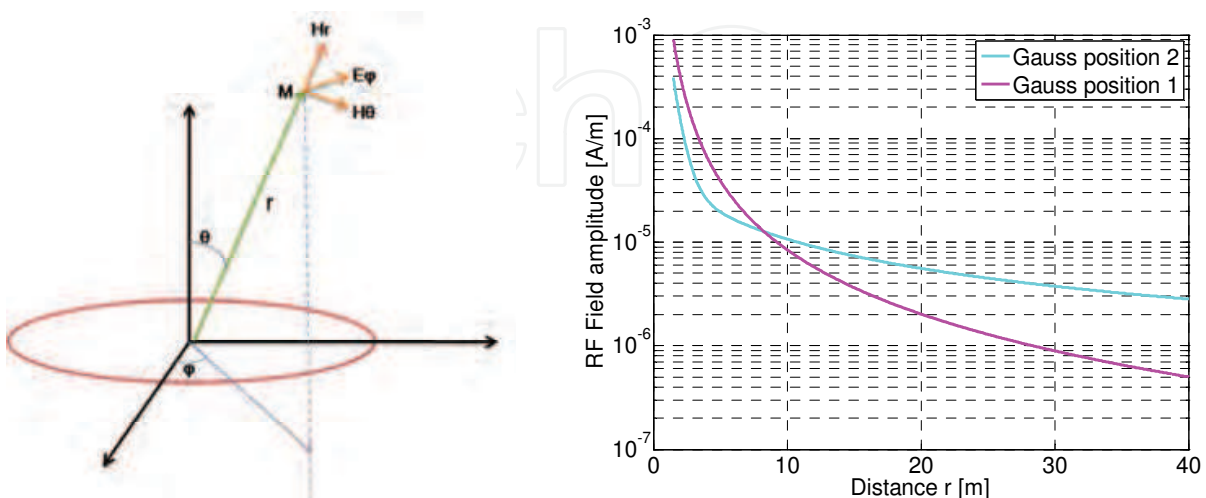


Fig. 2. a: Magnetic and electrical field seen as a distance r of the antenna; b: Results of the theoretical approach

Figure 3 gives the positions of the antennas in the case of the two positions de Gauss and conclude on their use in function of the eavesdropping distance. In the first Gauss position, an axis perpendicular to the reader antenna passes through the centre of the reader antenna and the spying antenna. In the second Gauss position, an axis parallel to the reader antenna passes through the centre of the reader antenna and the spying antenna.

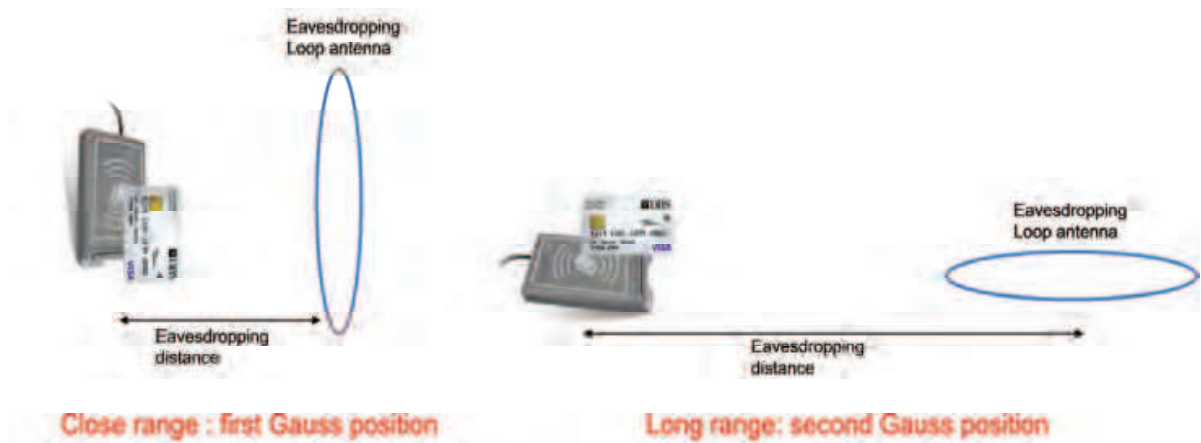


Fig. 3. Antennas positions for the two Gauss positions

3.3 Measurement protocol

Eavesdropping on a communication is a simple attack; a tuned antenna and an oscilloscope are sufficient to analyse signals transmitted between two contactless devices. Improvements on the signal processing can increase the eavesdropping distance. In these experiments, the reader and the card are products compliant to contactless ISO14443 standards; the reader is connected to a loop antenna compliant with the standard ISO10373-6 (ISO/IEC10373-6, 2011). The measured field at the centre of the reader antenna is 3.1A/m, i.e. the average range of the standard. Attacker antennas are one-turn inductive loop with a diameter of 30 and 50 cm tuned at 13.56MHz or 14.4 MHz (centred on the subcarrier frequency of the retro-modulated signal) and made with coaxial cable. The antenna signal is 60dB amplified, filtered with a band-pass filter at 13.56MHz and finally recorded on a scope (Figure 4).

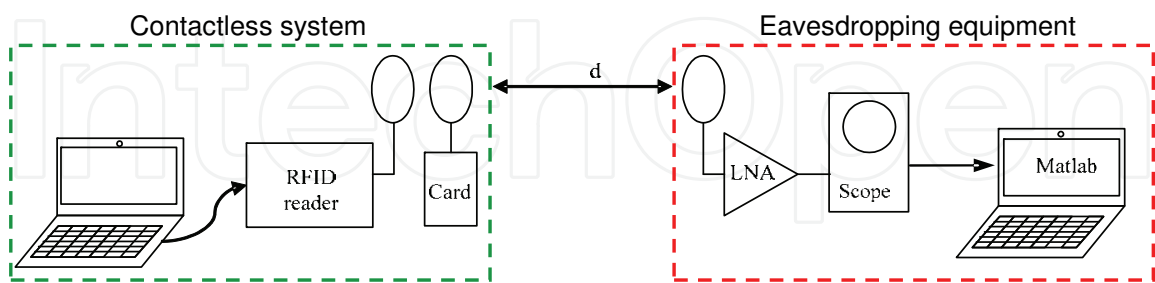


Fig. 4. Eavesdropping bench test

The recorded signals are then processed under Matlab: pass-band filtering, synchronous demodulation and detection (Figure 5).

3.4 Experiments

The forward and backward communication signals must be processed to recover a maximum of information. The contactless cards are passive, and the way to transmit data

from the card to the reader via the backward link is by the retro modulation of the reader signal. This implies that the distance to listen to the card is definitely smaller than for the forward link. The figure 6 gives an outline of analyzed signal. The forward communication can definitely be eavesdropped further because of the modulation used type.

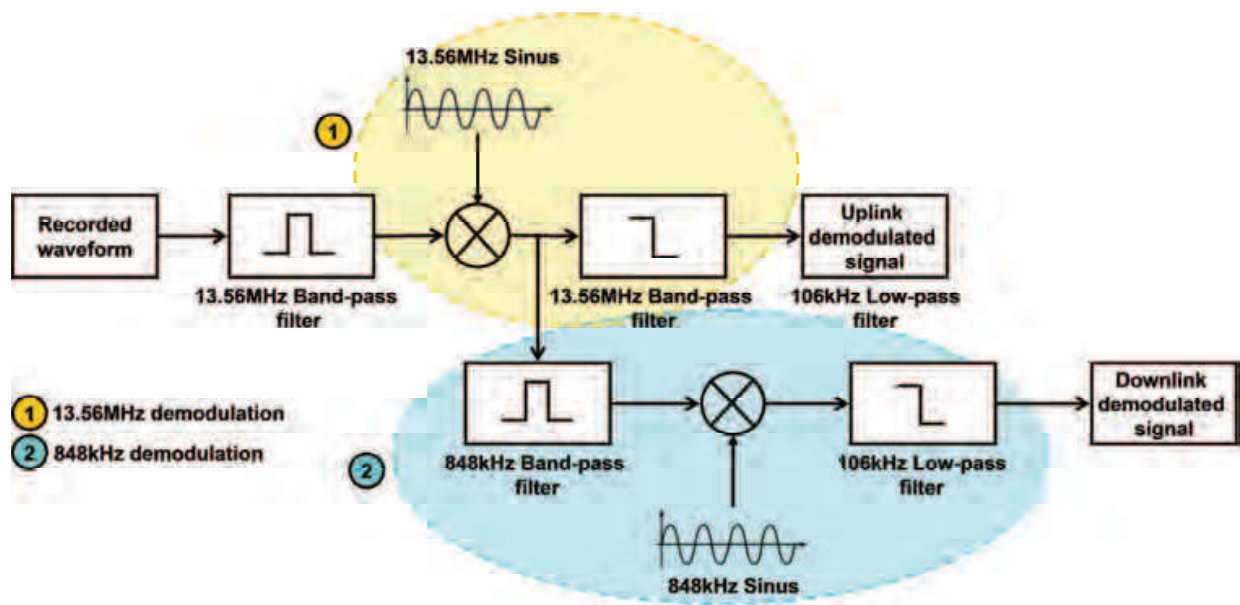


Fig. 5. Signal processing with Matlab

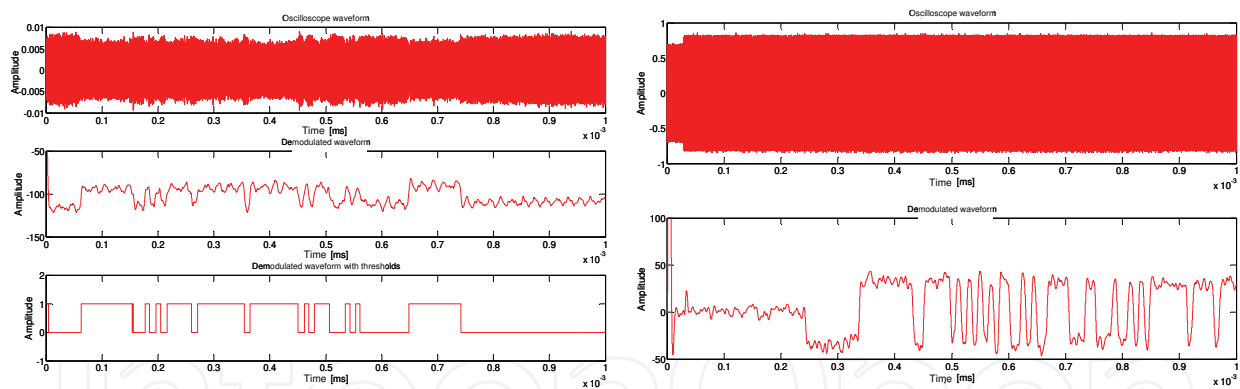


Fig. 6. Contactless forward communication link at d= 22 m and backward communication link at 3.5 m

A magnetic antenna will be used in the most of the realized experiments but the capability of using an electrical antenna to eavesdrop the HF signal gives information on the equipment that an attacker could use. A very simple antenna, an electric dipole has been used for this experiment. The results on the figure 7 show that the eavesdropping is noisier with an electrical antenna and that only the forward communication could be recovered at 4 metres.

First experiments on eavesdropping were realized in outdoor to avoid disturbances due to the environment. However, the attacker can not have a clean environment and it is important to understand the way in which an indoor environment can help an attacker to recover data. Two experiments were realized in indoor to answer to this question. During

the first experiment, an antenna, used in EAS (Electronic Article Surveillance) system, generates a rotating magnetic field. Then the RF field amplitude has been listed in few locations next to this antenna. It was demonstrated that signal voltage at the level of the antenna can be larger when the eavesdropping antenna is located further. In the same way, the second experiment was the analysis of the RF field of a badge antenna used in access control fixed on a laboratory door. It was possible to listen and record data several floors under in the lower part of the building with more than 8 m of vertical distance. After the analysis of these experiments, it was concluded that wirings, wall materials as reinforced concrete or metal framings of the doors appeared as very effective antennas relays.

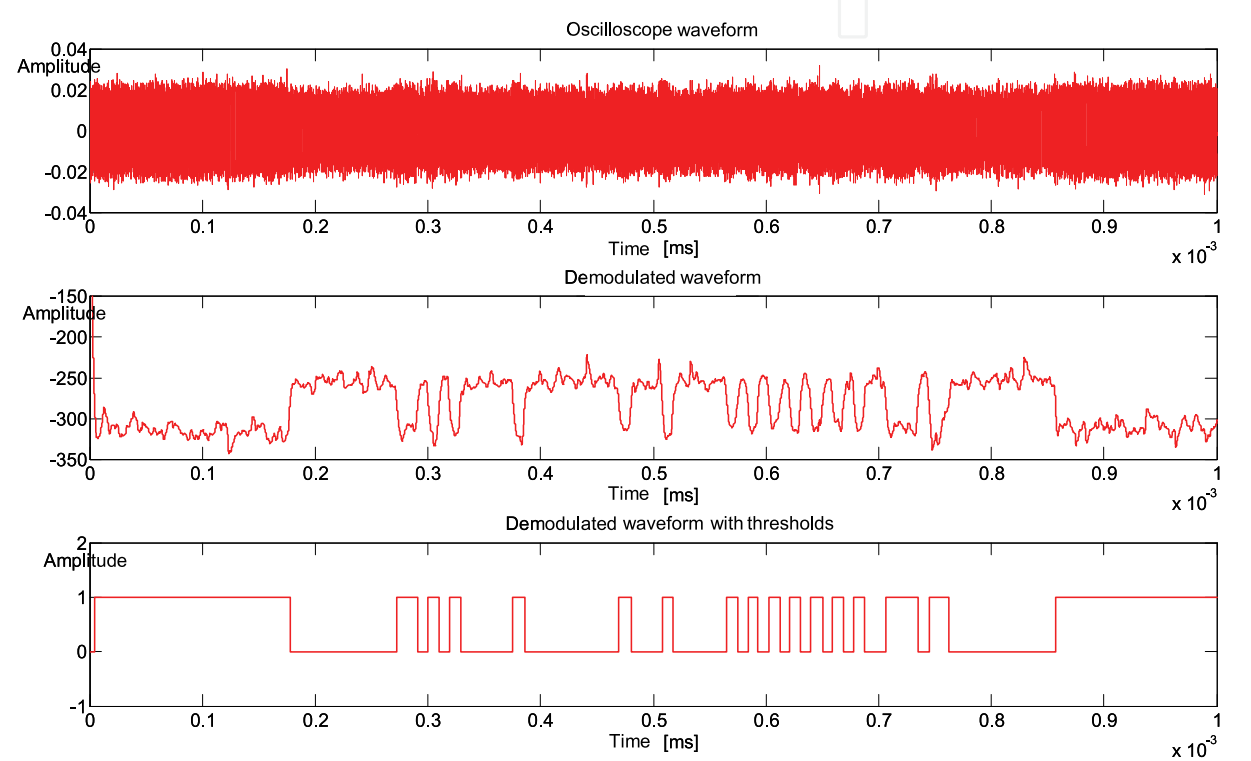


Fig. 7. Measured signals with an electric dipole at 4 metres from the emission

4. Skimming

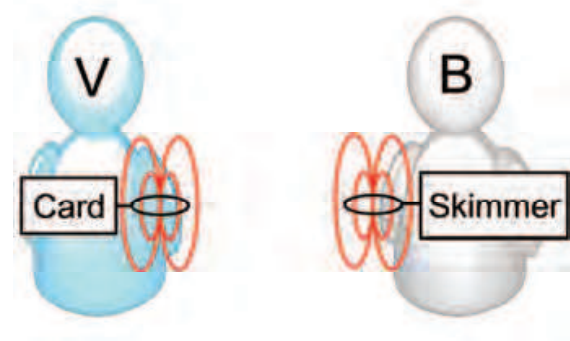


Fig. 8. Skimming attack

The skimming attack is to activate a card without its owner's agreement. In this active attack, the hacker needs to power the card, well modulates the field in the forward channel, and be capable to well process the load modulation of the backward channel in order to communicate with the card.

4.1 State of art

Many publications describe the features of the skimming attack. However only few of them describe practical scenarios or details of the experiments. Hancke has shown some interesting and detailed results on the skimming attack (Hancke, 2010). He has considered two different distances, the activation distance and the distance to retrieve the backward channel. Using different antenna sizes and different power levels, he has analysed different ways to activate the card and eavesdrop the communication. An important contribution of his paper is that the activation range do not increase in the same way as the distance of he could retrieve the token response. On the one hand, the best result of the retrieve distance was 2 m but with a skimming range of 15 cm. On the other hand he achieved a skimming range of 27 cm, however with less than 2 m of retrieval distance. In 2006, Kirschenbaum and Wool (Kirschenbaum & Wool, 2006), have already demonstrated almost the same skimming range. Using a cooper tube loop antenna and a power amplifier, they have demonstrated a theoretical and experimental setup to activate a card within a distance of 25 cm. Moreover, NXP (Tobergte & Bienert, 2007) has published that the skimming distance of ISO14443 systems is limited to approximately 30 cm. In addition, Kfir and Wool have demonstrated that beyond 50 cm the attack is hardly feasible, because the power requirements become increasingly important (Kfir & Wool, 2005). To conclude, lot of information is available about HF antennas. Application notes such as Texas antenna cook book (HF Antenna Cookbook) and Microchip antenna circuit design (Youbok, 1999), combined with some knowledge of ISO14443 systems, are enough information to know how to build a low cost skimmer device.

4.2 Theoretical study

4.2.1 Theoretical activation distance

Based on the Biot-Savart law, Equation 4 describes the link between the current I in a circular antenna and the magnetic field H function of the distance d between the reader and the transponder, r the radius of the circle and N the spires number of the antenna.

$$H(d) = \frac{r^2}{(r^2 + d^2)^{3/2}} \cdot N \cdot I \quad (4)$$

To keep the compliance with ISO standards, the field at the level of the transponder must be higher than 1.5 A/m. Figure 9 describes the behaviour of the field in the case of an antenna with one spire and 0.45 m radius parameters for different current in the circular loop.

Theoretical curves show that an attacker can hardly power and then activate a card situated at one metre from the reader.

4.2.2 Identifying the key parameters for the card activation

In order to identify the critical parameters, some aspects of the communication must be run through. The energy transfer can be improved and the attacker power optimized for a given frequency and communication range. Regarding RFID tokens which use high frequencies

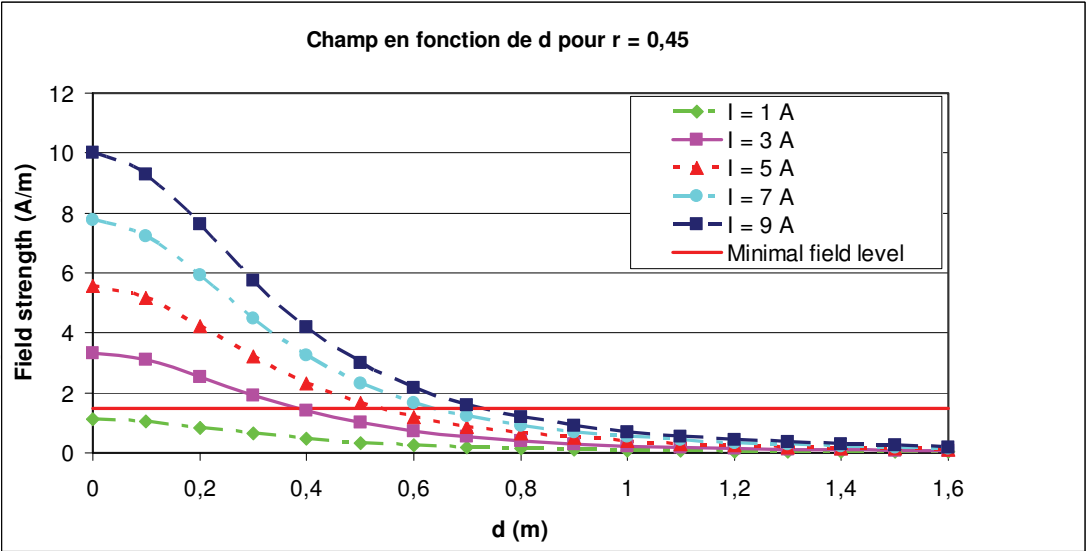


Fig. 9. Field amplitude versus distance between the reader and the transponder

and short range communication, the technique in this case is an inductive coupling. With the aim of activating the card, the hacker’s inductive antenna converts an electrical signal into a magnetic signal transmitted over the air. The interaction between the reader and the card is governed by the mutual inductance. The token will harvest all of its power from the energy emitted by the hacker’s antenna. Then, it can read, write and retransmit data through this magnetic field. Figure 10 describes the principle of coupling between two circuits with inductive loops.

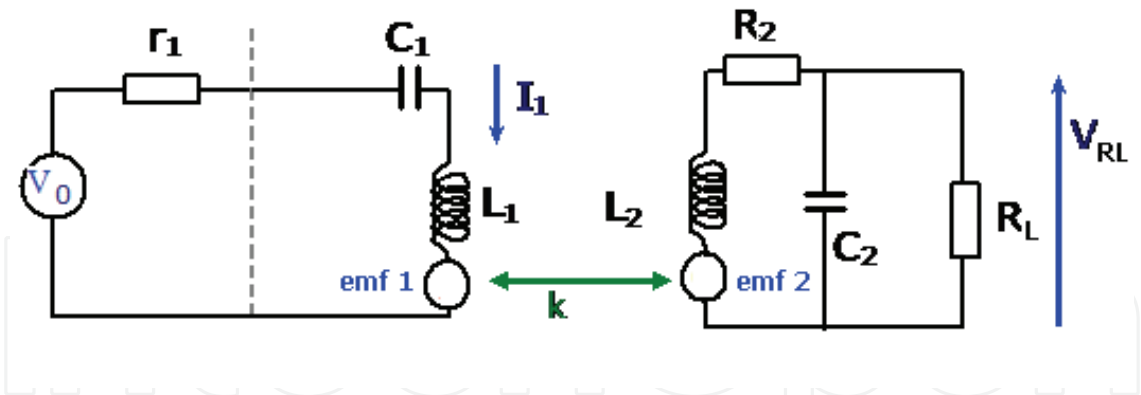


Fig. 10. Power transfer between the reader and the transponder

The mutual inductance between two circuits is defined as the ratio of the partial flux enclosed by the inductive loop of the card on the current I_1 passing through the loop of the reader (Reinhold, 1993)(Equation 5).

$$M_{12} = \frac{\psi_{12}(I_1)}{I_1} = \frac{\mu_0 N_2 H_1(I_1) A_2}{I_1}$$

(5)

Thus the mutual inductance between the antennas depends on many aspects of the card such as N_2 the number of turns in the card antenna, μ_0 the magnetic constant, and A_2 the area of the

card. It also strongly depends on the hacker's antenna field strength $H_1(I_1)$. To measure the efficiency of the coupling we use the coupling coefficient k , defined in Equation 6.

$$k = \frac{M_{12}}{\sqrt{L_1 L_2}} \quad (6)$$

Theoretical values of coupling coefficient could vary between the two worst cases $0 \leq k \leq 1$. However, in most of the standard HF RFID communications, the coupling coefficient average is close to 3%. (Finkenzeller, 2003).

As far as the coupling coefficient is greater than 0, an electromotive force emf will be created in the token circuit. This emf will empower the card and is calculated in the equation 7.

$$emf_2 = j\omega M_{12} I_1 \quad (7)$$

And the voltage across the load is given by the equation 8:

$$V_{RL} = \frac{j\omega M_{12} I_1}{1 + (j\omega L_2 + R_2) \cdot \left(\frac{1}{R_L} + j\omega C_2 \right)} \quad (8)$$

Most of the contactless card needs 10 mW to be activated. The Q factor of the circuit is defined in Equation 9 (Malherbi Martins et al., 2010).

$$Q = \frac{1}{\frac{R_2}{\omega L_2} + \frac{\omega L_2}{R_L}} \quad (9)$$

4.2.3 Improving the card activation

The main point for the hacker is to make the attack without being detected by the victim. Analysing the equations of the previous section, with the purpose to increase the operational range the hacker must increase the mutual inductance between his antenna and the victims token. In order to do that, he must increase his antenna power and the field strength emitted by it.

For each distance d , there is an optimal hacker antenna size. For typical forms of antenna, such as rectangular and circular antennas we can easily find the optimal radius r to obtain the maximum field strength H at a distance d (Youbok, 1999) (Equation 10).

$$H'(R) = \frac{d}{dR} H(R) \quad (10)$$

Using the optimal radius, the hacker increases the field strength H and the mutual inductance between his antenna and the victim's card.

To increase this power, the hacker will try to have the strongest current flowing through his antenna. For that, he will design his system with a high Q factor. However, this increase has a limit for two reasons. Firstly, a tuned circuit acts as a band pass filter, so with the purpose of recover the data of the backward channel, he must choose a compromise between power and bandwidth. For the ISO14443-A standard, the subcarrier is at 847 kHz, and the data rate

is 106kBits/s. In this way, the attacker must choose a low Q to maintain a high bandwidth BW (Equation 11).

$$Q \leq \frac{f_c}{2 \times BW}$$

(11)

Secondly, for different coupling coefficient values k there is an optimal Q factor for the antennas. The relation between the Q factor and k coefficient coupling is defined in the Equation 12:

$$n = k \cdot \sqrt{Q_2 Q_1}$$

(12)

For example a well designed antenna to activate a card at a distance d_1 could not activate a card at a distance d_2 . In fact, the activation distance depends of the value of n the system could have different behaviours.

For each value of n the system will has a specific coupling regime, as shown in the figure 11:

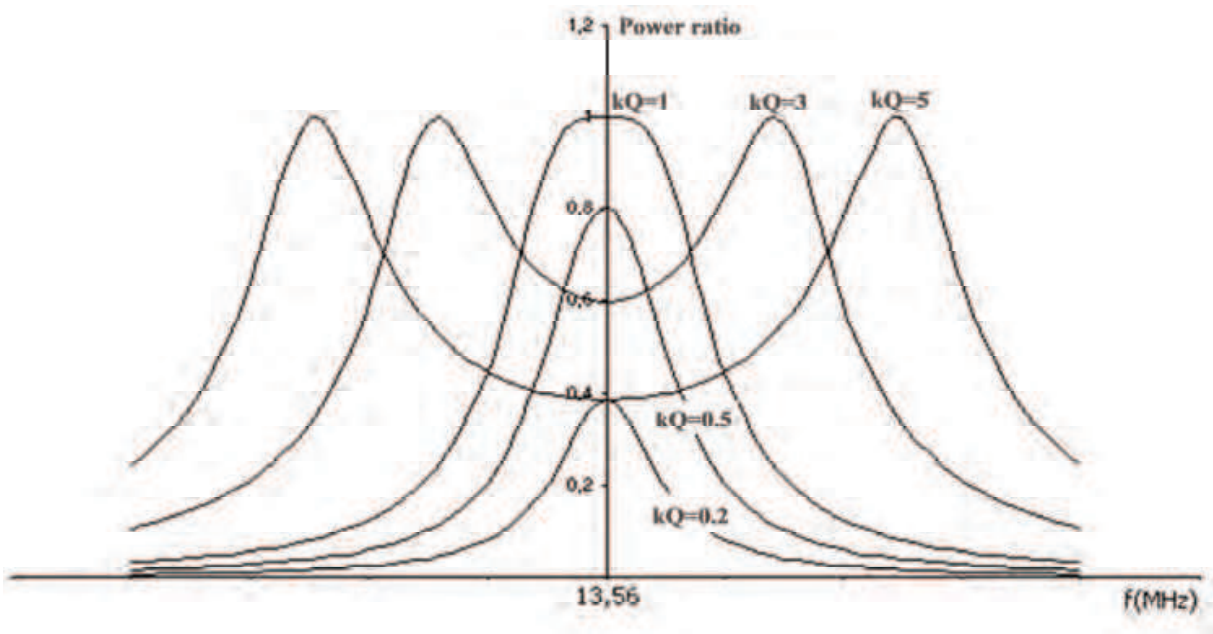


Fig. 11. The transferred power function of the product n

To have the maximum power across the R_L , the parameter “ n ” must be equal to 1. Using all these information a hacker could try to activate a card at important distances.

5. Relay and man-in-the-middle attack

The main objective of relay attacks consists in the setting of a communication between a true reader and a true contactless card. This attack is based on the Grand Master Chess problem described by Conway in 1976. The later shows how a person, who does not know the rules of this game, could win against one of two grand masters by challenging them in a same play. The relay attack is just an extension of this problem applied to the security field. By relaying information between a reader and a card outside the reader field, an attacker can circumvent the authentication protocol. This attack requires two devices, a mole which

pretends to be the true reader and a proxy which claims to be the true card. These two devices can communicate and thus relay data between the reader and the card. This communication can be wired or wireless.

Scenario:

In Japan or in USA, contactless systems are already used for payment applications. Under this scheme, an attacker can, by using relay attack, charges his purchases by a victim situated in the running area of the relay. To build this attack, the attacker is near the payment terminal and his accomplice near the victim. During the payment, the attacker places the proxy close to the payment terminal and the accomplice places the mole near the pocket of the victim; a relay is created between the terminal and the valid contactless card (Figure 12). The valid reader communicates with the card because it believes it is nearby him, so it debits the victim's account.



Fig. 12. Payment scenario: the relay attack setup

The man-in-the-middle attack is often mistaken for relay attack even if it is more advanced. The main features of the two attacks are the same: to allow the data transition through the relay between two wireless devices which are not in their communicating range. The distinctive feature is that the bits stream between the communicating devices can be modified during the relay by the attacker in the case of a man-in-the-middle attack.

5.1 State of art

5.1.1 Relay attack

To define the features of a relay attack, three different parts should be characterized: the mole, the proxy and the relay between them. The proxy acts as skimmer that has to activate and power the attacked contactless card and to communicate with it. Skimming a card is an attack as itself and is already discussed in this document.

The mole is able to eavesdrop on the communication with a real reader and to talk back to it. The eavesdropping on the communication is also well discussed in this document. Regarding the fake card response, active modulation could be used instead of a load modulation that requires a close coupling and so a short range.

The larger the distance between the different elements is, the more efficient is the relay. The theoretical maximum distance between the reader and the proxy is 50 m and 50 cm between the mole and the card. The distance between the mole and the proxy is not limited; it just depends on the used technology. (Kfir & Wool, 2005).

The wireless relay developed by Hancke can transmit requests and replies between an honest reader and an honest card separated by 50 metres (Hancke, 2005). The delay, introduced by such a relay is more than 15 μ s. However, many others communication channels can be used to link the mole and the proxy to increase the relay distance (Lishoy et al., 2010).

In (Oren & Wool, 2009), the authors have presented their work on relay attacks realized on an Israeli e-voting scheme. They have demonstrated that low-cost relays can compromise this system, the privacy and the security of voters. They have inserted a communication link between the voting terminal inside the voting booth and the ballot box that carried votes which were already cast. This attack permits to read, modify or suppress votes while the attacker is in the voting booth. It is carried out that relay attacks are easy to realize, difficult to detect and very dangerous for the privacy of data recorded on smartcards.

At the physical layer, this attack is the most dangerous for many reasons:

- With its capability of attacking from a long distance without the consent of the user and of bypassing the encryption of the contactless transaction, the relay attack appears to be one of the main threats for RFID systems. The card is activated and transmits information when it is powered, without the agreement of the victim. Anyone can be this victim because the attacker has just to be enough close to you to control your card.
- Relay attack is an attack on the physical layer; the relay transmits coded bits without knowledge about the frame significance. The ISO9798 standard describes an authentication protocol to prove that the actors of the communication know the secret key (ISO/IEC9798-3, 1998). For the eavesdropping or skimming attacks, the use of this kind of protocol limits the risks. For the relay attacks, it's not required to know this key. In fact, a relay does not modify information of the frame, and has not to know the frame meaning, it just transmits the data. The encrypted data are transmitted like a plain text.
- Contactless standards such as ISO14443 impose time constraints to synchronize data sent by many cards at the same time, particularly during the anti-collision protocol. However, these constraints are not enforced by the majority of cards. If we consider the ISO14443-A standard, the card shall reply after a precise time after the request. These requirements would complicate the relay attack if they are really applied. Carluccio et al. have realized have realized experiences which show that the reader accepts card reply starting within a time slice of 2.5 μ s every 9.44 μ s (Carluccio et al., 2006). Moreover, the token can specify the response time after its selection; this is the delay that a card can take to reply after a reader request. This time has a default value which is 4.8 ms and a theoretical maximum value of 5 s. These values let plenty of time to the attacker to relay the information and to modify the data in the relay too (Halvac & Rosa, 2007). Hancke et al. have presented results about experimental response timeouts; its value could be set to 19.7 s during the communication after the card selection (Hancke et al., 2009).

5.1.2 Man-in-the-middle attack

The man-in-the-middle attack is able to modify transmitted data without demodulating and decoding the signal (Verdult, 2008). However, this solution does not present much interest because it does not allow changing any bit for a specific coding and the attacker does not know the significance of its modifications. Another solution consists in demodulating and decoding the signal, analysing the frame and modifying this frame according to the data

that the attacker wants to transmit. By relaying information between a reader and a card without decoding the signal, an attacker can circumvent the authentication protocol; it is the main strength of the relay attack. The man-in-the-middle does not have this strength; the attacker has to know the frame significance to modify data. In the case of a ciphered communication, he must know the cryptographic algorithm and especially the secret key to decode the signal and discover its significance. The attacker knows the bits he can modified thanks to the decoded data. The new frame is then coded and modulated as a standard RFID signal. This attack is a real challenge if the attacker does not want to change arbitrary bits. Compared to relay attacks, the man in the middle attacks takes more time but the 5 seconds timeout defined by the ISO standard is enough to demodulate and compute any cryptographic algorithms.

5.2 Presentation of two new relays

The delay in current relays is mainly due to the use of components such as microcontrollers or RFID chips. This kind of components is used for the reconstruction of the decoded signals. Then, the original signal becomes compatible with other protocols, like Wifi or GSM, used in the wireless communication between the mole and the proxy. All these signal processes lead adding delays in the relay. Another solution is the use of analog components only. Attack scenarios with wired relays must be considered because they can introduce very low delays. Moreover, this kind of relays is simple to realize with few low-cost components. Even if they seem to be unlikely, they can be effective in a queue for example.

Passive wired relay: This attack consists of a coaxial cable of length l and an inductive antenna at each side, both matched and tuned at 13.56MHz (Figure 13a). The simple design allows very low delays. This delay is due to the length of the cable and the establishment time of the signal. This attack is a major threat because the delay may be less than a period of the 13.56 MHz carrier.

Wireless super heterodyne system: This relay, shown on figure 13b, is quite similar to the relay attack developed by Hancke because it is not restricted by a wired link. Unlike Hancke's relay, our wireless relay does not use digital components such as microcontrollers or RFID chips to process the signal. The delay introduced by this relay should be shorter. To do so, the reader signal of frequency f_c is mixed with another signal of frequency F , generated by a local oscillator. It results a signal of frequency $f_c + F$, easier to amplify and to send further. A PLL is used as a local oscillator to have the same frequency in the modulation and demodulation circuit.

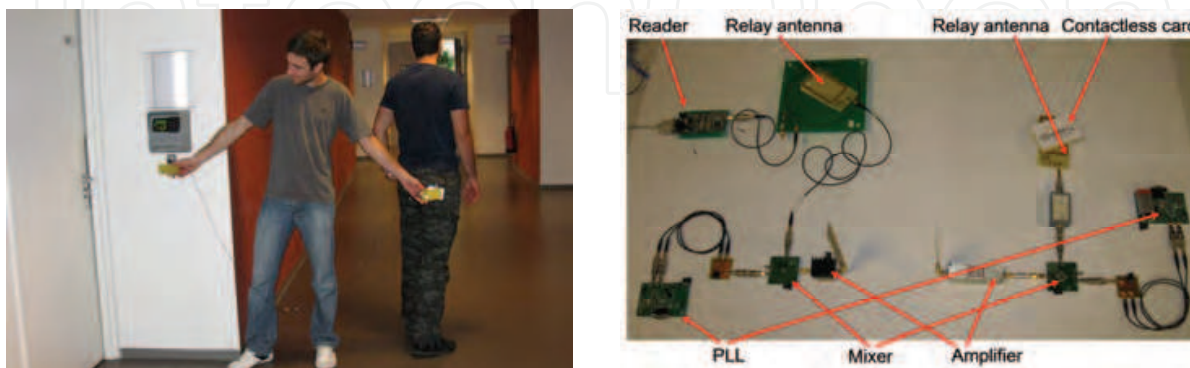


Fig. 13. a: Potential use of a wired relay in a hallway, an attacker creates a relay between an access terminal and a true contactless card; b: Experimental setup of the uplink system of a wireless relay

5.3 Experiments on relays

Two different experiments were realized. The first was to prove that all these relays work and to determinate their characteristics such as complexity, cost or values based on their performances. The delays introduced by these relays are so short that it is not possible to determinate them with unaided eye and it is necessary to use signals with precise properties to correlate them. For that, the second experience has for objective to measure values of these delays with the best accuracy. For all these tests, our reference is the relay developed by Hancke which is the most detailed in the literature (Hancke, 2005).

The bench test is roughly the same for the two experiments; the reader is connected to the computer in order to send commands, the card is placed few meters away of the reader. A relay is positioned between the reader antenna and the card. Two calibration coils are placed up on either side of the relay; they allow visualizing and recording signals on the oscilloscope.

5.3.1 Demonstration of relay efficiency

For these tests, only equipment compliant with the standard ISO14443-A is used because the main objective is to prove that our systems can relay data between a true reader and a true card (Figure 14). The reader is connected to an antenna conform to the ISO standard which has a quality factor of 10.

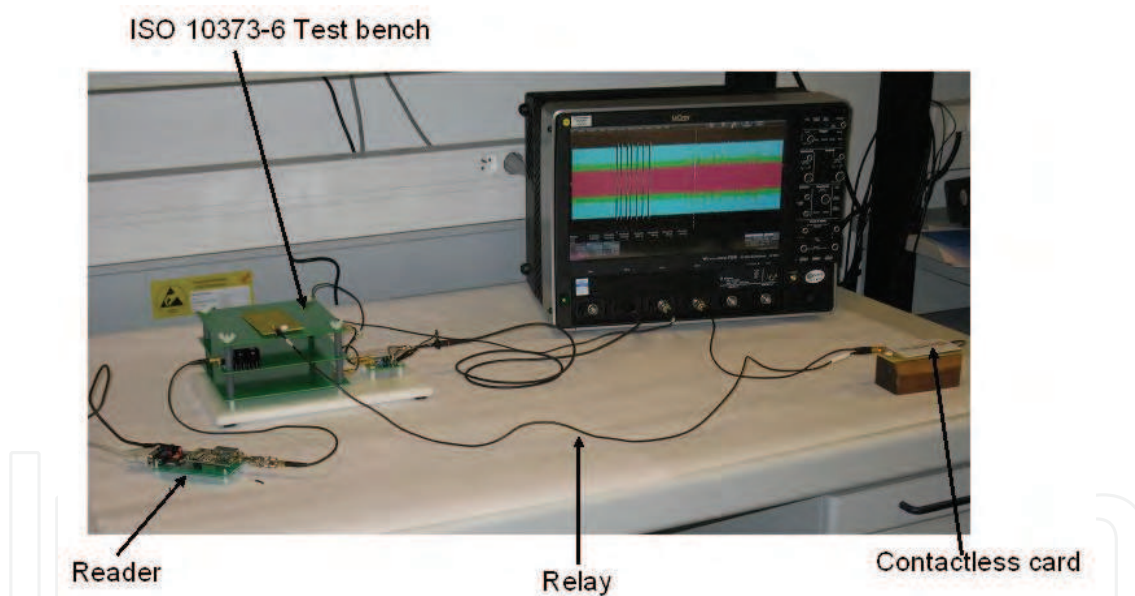


Fig. 14. Test for the wired relay: experimental setup to measure the load modulation amplitude

It is possible to vary different parameters such as the physical length of the relay, the distance between the reader and the proxy or the distance between the card and the mole. Varying the distance reader-proxy is not really interesting because the attacker could put the proxy as near to the reader antenna as he can. Conversely, the mole-card distance is an important indication on the relay performance as the attacker can not really control the distance between his mole and the card he wants to activate. For each relay attack, we focus on the maximum distance of activation of the card. For a contactless system without relay, the activation distance is close to 10 cm

The cost and the complexity are important to determine the resources an attacker need to put in place a relay attack.

The ISO standard imposes a load modulation amplitude at least $30/H^{1.2}$ (mV peak) where H is the (rms) value of magnetic field strength in A/m (ISO/IEC14443-2, 2001). In our test, the value of H is 2A/m so the load modulation shall be superior to 13 mVp rms. Our two relays have load modulation amplitude higher than the standard level, which proves they are in accordance with this standard and undetectable by a subcarrier amplitude computation method. The table 1 summarizes all the results of the experiments realized on relay attacks.

5.3.2 Delay measurements

The main objective of the second experience is to measure the delays introduced by the two described relays using correlation computation. Measuring delays close to the period of the subcarrier is difficult with a standard contactless system so we have used an open reader that we developed. With this reader, it was possible to send signal with specific modulation properties easier to correlate. The reader sends a fixed signal through a relay; this signal is recorded directly on two calibration coils located close to the two relay antennas.

This experience is reproduced for different coupling between the reader antenna and the first antenna of the relay. To vary the coupling between the antennas, we increase the distance between them; 3 distances are chosen: 1, 3 and 8 cm.

		Contactless system with relay				Contactless system
		Wired relay	Wireless relay	Hancke's relay		
Cost		*	****	***		
Complexity		*	****	****		
Activation distance		4.5 cm	5 cm	No data		
Load modulation (mVp)		14.17	14	No data		10 cm
Relay maximum length		> 10 m	> 50 m	50 m		> 13 mVp rms
Distance reader antenna – relay antenna						
delay	1 cm	295 ns	566 ns	15 μ s		
	3 cm	442 ns	454 ns			
	8 cm	442 ns	652 ns			

Table 1. Characteristics for each relay

The correlation of the two recorded signals permits to compute the temporal shift between them. Results in table 1 show that the delay sometimes decreases for a same relay when the distance increases between its antennas. Generally, the delay in a contactless system depends on three parameters: the establishing time in antennas which is function of the bandwidth, the propagation time in the air and the signal processing in case of relay presence. The propagation time in the air is short, i.e. less than 300 ps. The important parameter is the establishing time of the modulation amplitude variations which strongly depends on the coupling between the two antennas and of the bandwidth of the antenna,

i.e. the quality factor. This factor can introduce disparities in the cross-correlation computation.

Figure 15 gives a global view of the computed delays. Each type of relay is characterized by a time distribution. Wireless relays and wired relays have roughly the same delays because the mix of the signals is very fast. The computed delay for the relay developed by Hancke is more important than the others due to the time duration of each step of the signal processing.

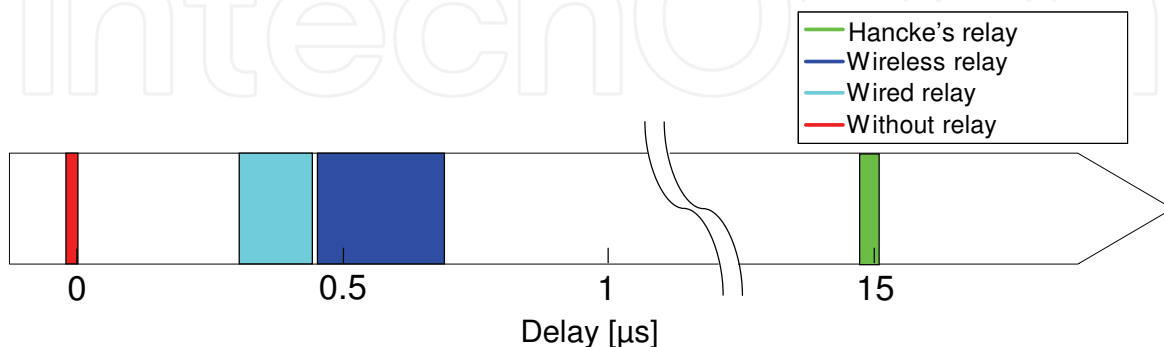


Fig. 15. Computed delays with correlation technique versus delay introduced by hancke's relay

6. Denial of service

The goal of denial of service attacks is to somehow deny a given service (e.g. identification) to valid users. Denial of service attacks are easy to accomplish and difficult to guard against. They can be divided into the four categories:

- Interferences in the anti-collision protocols
- Reader- and card jamming
- Faraday cage
- Destruction or deactivation

6.1 Interferences in the anti-collision protocols

Anti-collision protocol is an algorithm which avoids the communication of different cards in the same time. A reader is not able to decode data from multiple sources. To manage the collision of transponders, there exist two different protocols: a probabilistic protocol and a deterministic one. These protocols can be used as denial of service device by forbidding the access at one or many transponders.

6.1.1 Deterministic protocol: the Tree Walking algorithm (ISO/IEC14443-3, 2001)

This protocol is able to calculate the exact time required by the reader to know the UID (Unique Identifier) of every tag depending on the number of tags in the reader field. All possible UID can be viewed as the leaves of a binary tree of depth equal at the UID bit length. The reader initiates the singulation protocol at the root of the binary tree and requests the UID of all tags in its field. A collision occurs when two tags simultaneously send a different bit. In this case, the tree-walking interrupts on the child collision node. Then, the reader requests all tags with an UID starting by the bits recorded before the

collision to start at the previous node and selects the next branch '0' or '1'. Only tags with UID starting with this bit path reply to the reader. If another collision occurs, the reader repeats the last sequence until it obtained a complete UID (Figure 16).

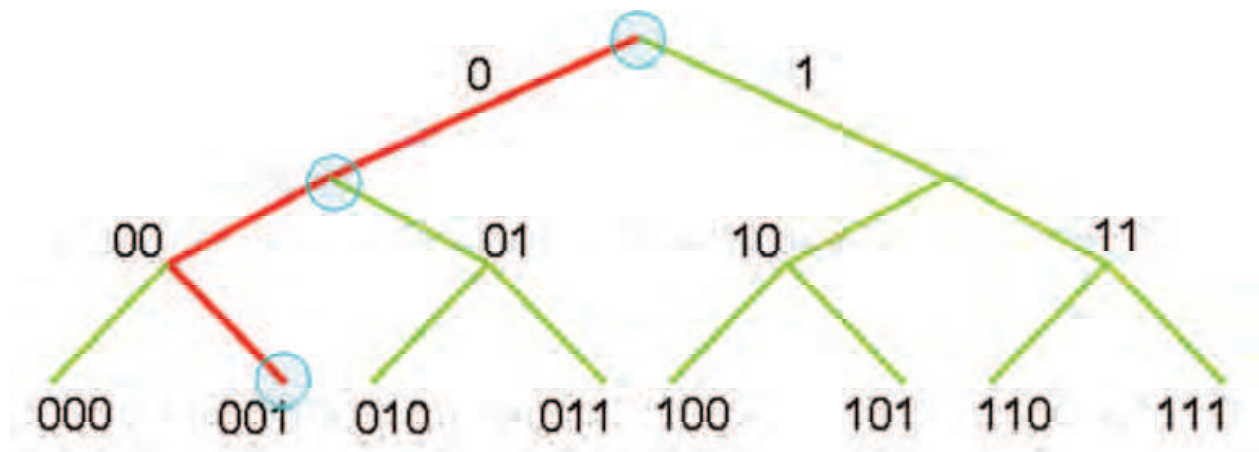


Fig. 16. Tree Walking for a 3-bit UID to obtain the "001" UID

The blocker tag is a device developed by Juels et al. to block the tree walking protocol and then prevent your card access by an intrusive reader (Juels et al., 2003). To jam the protocol, the blocker tag simulates a real tag and emits both '0' and '1' (which requires two antennas) at each reader anti-collision request. This creates a collision and the reader can not complete the algorithm and find out the tags UID. In most cases, such a device is used by the consumer to protect against unwanted scanning. However, the blocker tag can be used by an attacker to generate a denial of service in a legitimate system. We can even assume that a blocker tag is always malicious since it cannot be selective and forbids the reading of one tag whereas it authorizes the reading of others.

The attack is area limited since the blocker tag acts as a passive tag. It needs to be in the reader field to operate. Then it must be located close to the reader to have the best efficiency. However, an active tag can be realized to improve the blocking area of the system.

6.1.2 Probabilistic protocol: the Aloha method (ISO/IEC14443-3, 2001)

The second protocol assesses the probability to obtain the UIDs of a certain number of tags in a given time without giving any guarantee concerning its maximum value. This algorithm is known as time slots or Aloha method. The principle is simple: each tag can reply to the reader in fixed time slots during one or many rounds. A time slot is a period of time during one or more tags can reply. At the beginning of the first round of the anti-collision protocol, the reader sends the number of time slots used during the round. A tag can only reply during an single random time slot in a same round. The reader analyses each time slot:

- When a tag is alone to reply during a time slot, the reader retrieves and records its UID.
- When at least two tags reply during the same time slot, there is a collision.

If there is at least one collision during a round, the reader must throw again a new round without identified tags. Then, during the new round, the probability that two tags reply in the same time slot is lower. The reader throws again rounds until there is no collision during a round and the reader has the UID of all tags in its field.

An attacker can use the weaknesses of this anti-collision protocol to jam it and block the communication between the reader and the card. The principle is close to the blocking protocol of the Tree-walking algorithm. As the reader creates a new round if a collision occurs during one, an attacker just has to create a collision during each round. In each time slot of a round, the attacker simulates a tag and sends a random UID. The reader is blocked in its anti-collision protocol and it can not collect UID cards (Figure 17).

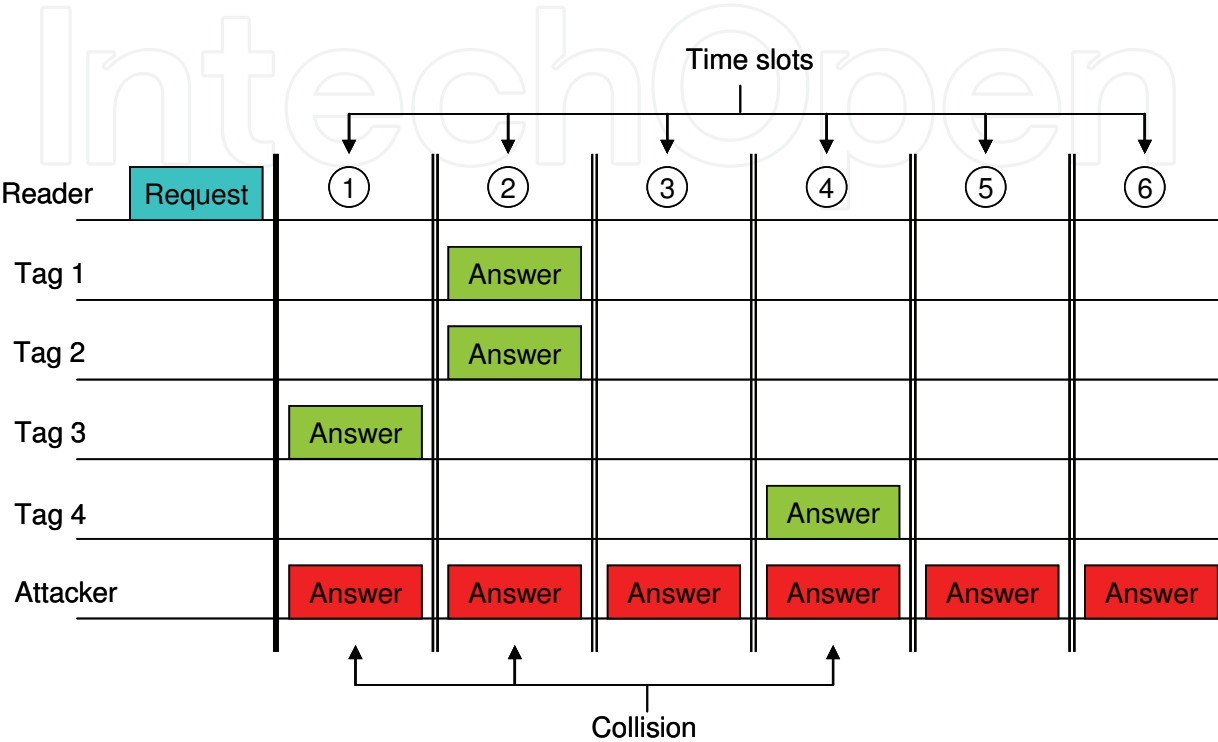


Fig. 17. Blocking protocol for Aloha method

6.2 Reader and card jamming

Jamming is an attack by denial of service which consists in emitting a signal in the same bandwidth as the reader and the card in order to blur the communication between the reader and the card. The only constraint is to flood the reader or tag signal in a higher level noise. The maximal level of emitted magnetic field is defined by ETSI (European Telecommunications Standards Institute) legislations. The ETSI EN300-330 describes a template of magnetic emission at 10 m around 13.56 MHz (ETSI 300-330). According to the following figure, it is illegal to emit more than 42 dBμA/m at 10 m in the 13.56 MHz close range frequency (Figure 18).

As a consequence, any attacker that is able to go over this limitation is sure to create an efficient jamming of an RFID reader. Exceeding the standard value does not necessarily mean that the jamming signal requires a lot of power. If the noisy emission is in the exact bandwidth of the reader signal, only few watts (1 to 2 W) are enough. To blur a tag signal is even easier since its signal is much lower than the reader's.

6.3 Shielding and Faraday cage

Magnetic field can be blocked or dramatically reduced by the process of shielding. It consists in confining an object in a metallic sheet with properties able to stop

electromagnetic waves. To prevent the reading of a contactless card by a reader, its owner can insert it in a specific wallet made of metallic sheet (Figure 19). This wallet plays the part

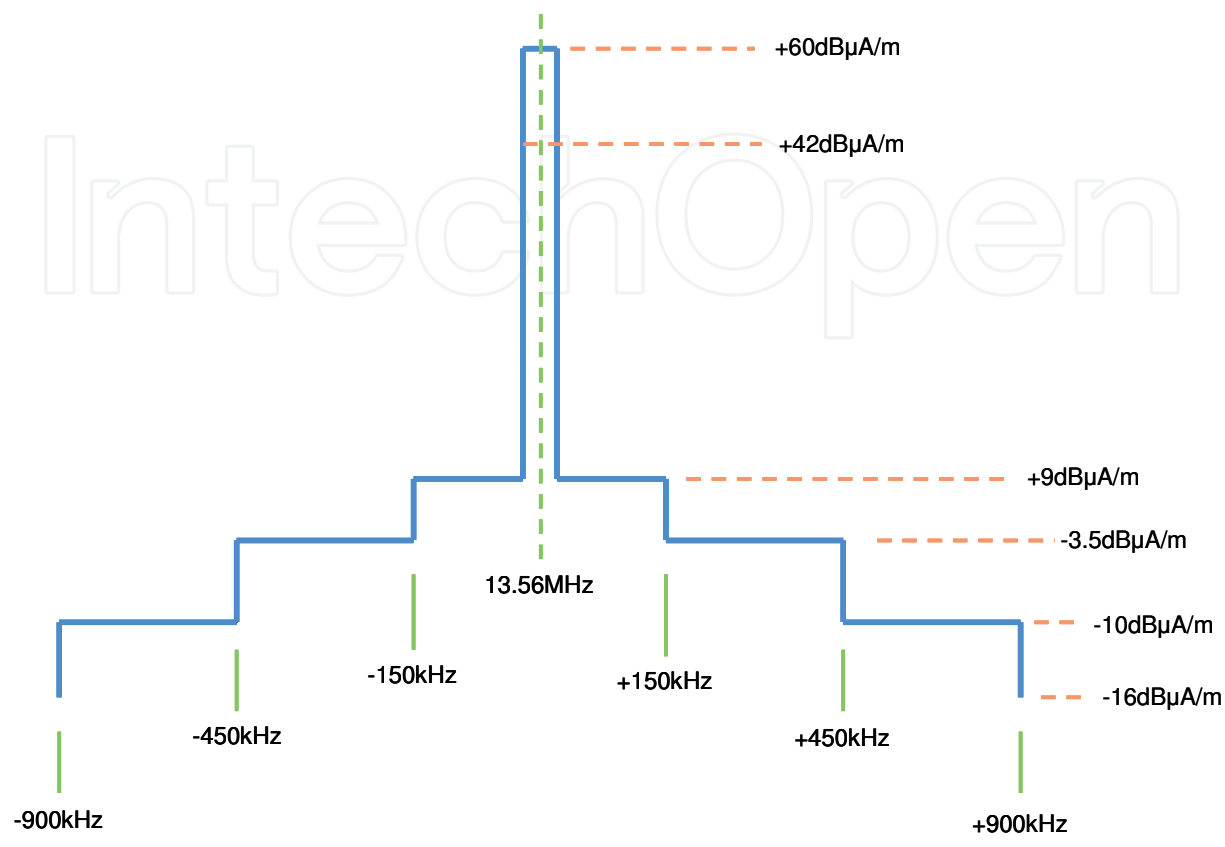


Fig. 18. ETSI EN300-330 13.56 MHz: Maximal magnetic field at 10m from the reader

of a Faraday cage blocking all HF and UHF radio signals of readers. This solution is a counter-measure to avoid the spying of confidential data recorded on cards by a false reader. However, this solution can be used to make denial of service. For example, an attacker can pass through detection system by shielding RFID EAS (Electronic Article Surveillance) to not pay its purchases.

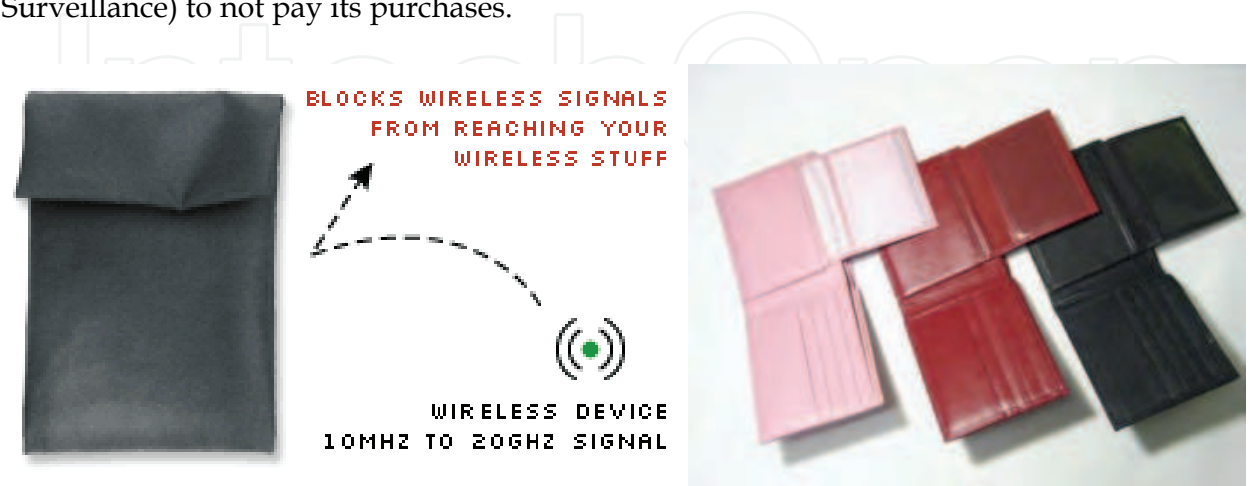


Fig. 19. Such systems block radio communications in the frequency range 10MHz-20GHz (MobileCloak), (DIRFwear)

6.4 Destruction or deactivation

This attack consists in making definitively unusable a contactless card, but it can concern the reader, too. Although this attack threatens contactless system availability, it is different from the denial of service attack because once performed, it is irreversible. Destruction is considered as an attack when it is practiced without the holder’s consent but it is privacy protection if a card is definitively destroyed with the consent of its holder in order to protect its data from any future attacks. Only physical destructions are treated in this chapter dedicated on physical attacks.

6.4.1 Destruction by electromagnetic field

In the same way that a chip can be damaged when powered by a forbidden voltage, the chip of a transponder can be destroyed. In fact, the chip of a card is powered by the magnetic field on the transponder antenna. The chips could not resist to a high level magnetic field. This attack is mainly efficient with inductive loop contactless devices. If the inducted voltage in the loop antenna exceeds a certain value, then the chip can be definitely damaged. This value depends on chip features and on its developers but a 12A/m magnetic field is generally large enough to destruct RFID chip. The strength of this attack is that there is no absolute protection against destruction by electromagnetic field.

Protections, such as Zener diodes or self-heating fuses, can be integrated. However, their protection effect is limited by the available chip area. This attack can be very dangerous in the case of contactless passport or ID card destruction. On the other hand, generating a strong magnetic field requires a large instrumentation and a significant power (BSI, 2004). Then, an attacker is not able to destruct one or many transponders in the same time if they are far away from him.

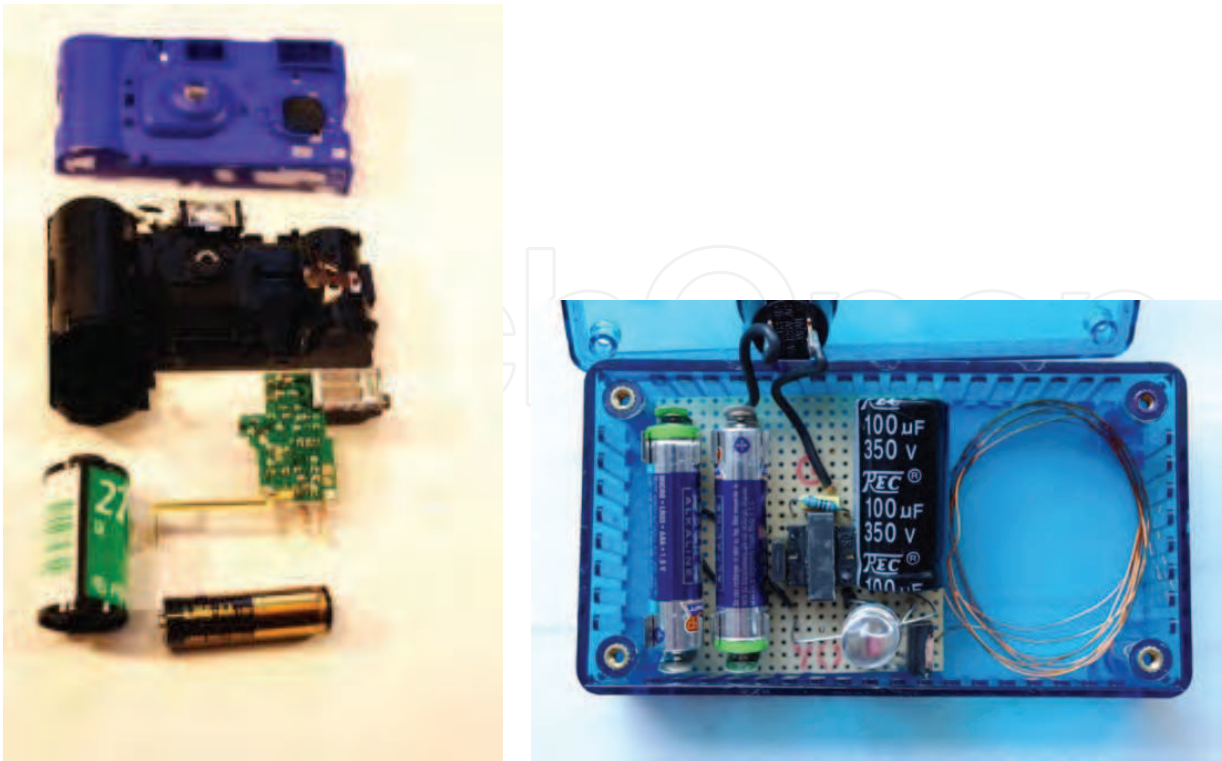


Fig. 20. Examples of RFID transponders killer (RFIDzapper (EN), 2006), (RFIDzapper)

Building its own RFID transponders destroyer is not a challenge because many websites present schematics and practical implementations. For example, the RFID zapper is a home-made device able to destruct or definitely deactivate close RFID chips. It generates strong electromagnetic pulses by using the electronic of a camera flash and of a power generator. The principle is simple: the generator charges a large value capacitor and the flash is substituted by a simple coil. The discharge of the capacitor generates a strong concentration of energy comparable to an EMP (Electro Magnetic Pulse). The RFID zapper is only an example of devices found on the web but there exists complete devices with tag detector (Figure 20).

The microwave is another way to destruct RFID tags but it can hardly be used by an attacker because this attack needs the access of the cards he want to kill.

6.4.2 Mechanical or chemical destruction

A transponder is usually composed of an antenna and a chip: these two elements can be viewed as two mechanical pieces. The first is just made of a thin copper strip and the chip is fragile and protected by a plastic packaging. It exists many solutions to destruct the transponder. The major part of methods leaves visible signs of damage and needs the access of the card. For example, the inductive antenna is vulnerable; an attacker can easily cut it with scissors. As the antenna is essential to recover power and data, the transponder does not run anymore with a cut antenna. However, an attacker can also destruct a transponder without giving clue on an intentional damage. A solution is to cut the antenna very close to the chip or to hit the chip with a hammer in the case of an unpackaged tag (Instructables, 2008).

7. Substitution, counterfeiting, and replay attack

These three attacks are described in the same part because of they have mainly the same principles. All these attacks need the steal of data from another card. Skimming or eavesdropping attacks allow the dumping of main information recorded in the memory of the attacked chip. In this case, the attacker can store the stolen data in a blank contactless card to have a clone of the attacked card. Write data on a blank tag is not a challenge as anybody can easily buy on the Internet any card from any manufacturer that has a microprocessor which can be easily programmed (DN-Systems, 2007 as cited in Mitrokotsa & al., 2008). Another way is the steal of a contactless card directly on its owner by using violence. In the two cases, the attacker obtains a card with new UID and recorded data. These leads to the three attacks: substitution, counterfeiting and replay attacks.

It is also possible to substitute a RFID tag on an item with another tag of a cheaper item or with a tag that is totally reprogrammed with an aforementioned chip

The replay attack consists to send to a true contactless card or reader, sequences recovered during an eavesdropping or skimming session with a true reader or card. This attack allows the possibility to have transactions without a true card or reader. Grunwald shows its skills at cloning an e-passport, that means a terrorist can pass a frontier with a fake identity (Zetter, 2006).

8. Conclusion

This chapter presents a comprehensive overview of the main attacks on the HF physical layer of contactless technologies. These technologies use radiofrequency waves to transmit

data and power between two devices. This communication medium can be exploited by an attacker and then reduce the security and privacy of the card user. The growth of this technology in critical domains such as payments is slowed down because of all the threats which can occur on the card and its user. They do not trust in this technology since it is not secure in terms of confidentiality and privacy of data exchange. Payment smartcards were already a potential source of attacks but the user had a complete control thanks to use of a confidential code and the insertion of the card in the cash dispenser. This weakness can be used in the case of the skimming attack to activate a card as a valid user without the agreement of the card owner. The use of radiofrequency waves disables the management of the communication by the card user. In addition to that, the propagation of the electromagnetic waves in the air enables attacks like eavesdropping. Contactless systems, according to ISO14443-A and B standards, have an operating distance of a dozen of centimetres. However, the experiments and the state of art show that an attacker can eavesdrop a private communication from a reader to a card up to 20 metres. A communication from the card to the reader can be listened at a distance less than 5 metres. Moreover, the use of metallic materials, cables, walls and doors is a great opportunity for attackers as the metal acts as antennas. The major threat is an attack combining the basics of the eavesdropping and skimming attacks. An attacker can create a communication relay between two contactless devices which are not in their communication range. This attack can be used with smartcards but is powered by the use of the air medium. Although the operation distance is close to the dozen of centimetres, an attacker can establish a communication between two devices without distance limit. Basic relay attacks are developed to point out that relay attacks can add delay less than 1 μ s. The weakness of the air medium is used in a denial of service of the devices to blur the communication by causing fail the anti-collision protocols or by flooding the reader and the card signals. The destruction of the devices or their placement in a faraday cage can also be considered as a denial of service. Most of these attacks can reveal secret information which can introduce attacks like replay or cloning attacks. This overview permits to show the main threats of this technology in terms of security and privacy. It is necessary to develop methods and technologies in order to make these systems more secure and their use more confident.

9. References

- BSI (2004). Security Aspects and Prospective Applications of RFID Systems; Federal Office for Information Security, 2004
- Carluccio D., Kasper T. & Paar C. (2006). Implementation details of a multipurpose ISO 14443 RFID-tool, Proceedings of RFIDsec'06 Workshop on RFID Security, Graz, Austria July 12-14, 2006
- DIFRwear , DIFRwear's RFID Blocking Products, 17.02.11, Available from: <http://difrwear.com/>
- DN-Systems (2007). BBC Reports on Cloning of the new e-passport, 17.02.11, Available from: <http://www.dnsystems.de/press/document.2007-01-04.2112016470>,
- ETSI300-330. Electromagnetic compatibility and Radio spectrum Matters (ERM); Short Range Devices (SRD); Radio equipment in the frequency range 9 kHz to 25 MHz and inductive loop systems in the frequency range 9 kHz to 30 MHz, 17.02.11,

- Available from:
<http://www.etsi.org/website/Technologies/ShortRangeDevices.aspx>
- Finke T., Kelter H. (2004). Abhörmöglichkeiten der Kommunikation zwischen Lesegerät und Transponder am Beispiel eines ISO14443-Systems, BSI
- Finkenzeller K. (2003). RFID Handbook Fundamentals and Applications in Contactless Smart Cards and Identification 2nd Ed., John Wiley & Sons, Ltd, pp. 434, ISBN: 0-470-84402-7, Munich, Germany, 2003
- FOIS(Federal Office for Information Security) (2004). Security Aspects and Prospective Applications of RFID Systems
- Guerrieri J. & Novotny D. (2006). HF RFID eavesdropping and jamming test, Electromagnetics division and Electrical Engineering Laboratory, NIST Internal Report 818-7-71
- Halvac M. & Rosa T. (2007) A Note on the Relay Attacks on e-passports: The Case of Czech e-passports, IACR Cryptology ePrint Archive, Report 2007/244
- Hancke GP. (2005). A Practical Relay Attack on ISO 14443 Proximity Cards, In: Gerhard Hancke homepage, 17.02.11, Available from:
<http://www.rfidblog.org.uk/research.html>
- Hancke GP. (2006). Practical attacks on proximity identification systems, Proceedings of S&P'06 IEEE Symposium on Security and Privacy, ISBN 0-7695-2574-1, Oakland, California, USA, May 21-24, 2006
- Hancke GP. (2008). Security of Proximity Identification Systems. PhD thesis, University of Cambridge, Cambridge, United Kingdom, February, 2008
- Hancke GP. (2008). Eavesdropping Attacks on High-Frequency RFID Tokens, Proceedings of RFIDsec'06 Workshop on RFID Security, Budapest, Hungary, July 9-11, 2008
- Hancke GP., Mayes K. & Markantonakis K. (2009). Confidence in Smart Token Proximity: Relay Attacks Revisited, Elsevier Computers & Security, Vol. 28, Issue 7, pp. 615-627
- Hancke GP. (2010). Some practical results and discussion of related industrial and academic work on eavesdropping and skimming attacks, Journal of Computer Security
- Hoshida J. (2004), Tests reveal e-passport security flaw, In: EETimes, 17.02.11, Available from: <http://www.eetimes.com/showArticle.jhtml?articleID=45400010>
- Instructables (2008). How to block/kill RFID chips, In: Instructables, 17.02.11, Available from: <http://www.instructables.com/id/How-to-blockkill-RFID-chips/step4/How-to-kill-your-RFID-chip/>
- ISO/IEC14443-2 (2001). Contactless integrated circuit(s) cards -- Proximity cards -- Part 2: Radio frequency power and signal interface, ISO (International Organization for Standardization), Geneva, Switzerland
- ISO/IEC14443-3 (2001). Identification cards -- Contactless integrated circuit(s) cards -- Proximity cards -- Part 3: Initialization and anticollision, ISO (International Organization for Standardization), Geneva, Switzerland
- ISO/IEC10373-6 (2011). Identification cards -- Test methods -- Part 6: Proximity cards, ISO (International Organization for Standardization), Geneva, Switzerland

- ISO/IEC9798-3 (1998). Information technology -- Security techniques -- Entity authentication -- Part 3: Mechanisms using digital signature techniques, ISO (International Organization for Standardization), Geneva, Switzerland
- Juels A., Rivest R. & Szydlo M. (2003). The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy, Proceedings of CCS 2003 Conference on Computer and Communications Security, pp. 103-111, ACM Press, Washington, USA, October, 2003
- Kfir Z. & Wool A. (2005). Picking virtual pockets using relay attacks on contactless smartcard systems, Proceedings of SecureComm 2005 Conference on Security and Privacy for Emerging Areas in Communication Networks , pp. 47-58, ISBN 0-7695-2369-2, Athens, Greece, September 5-9, 2005
- Kirschenbaum I. & Wool A. (2006). How to Build a Low-Cost, Extended-Range RFID Skimmer, IACR Cryptology ePrint Archive, Report 2006/054
- Lishoy F., Hancke GP., Mayes K. & Markantonakis K. (2010). Practical NFC Peer-to-Peer Relay Attack using Mobile Phones, Proceedings of RFIDSec'10 Workshop on RFID Security, pp. 35-49, ISBN 978-3-642-16821-5, Istanbul, Turkey, June 7-9, 2010
- Malherbi-Martins R., Bacquet S., Reverdy J. (2010). Multiple loop against skimming attack. Proceedings of Fifth International Conference on Systems and Networks Communications (ICSNC) , ISBN: 978-1-4244-7789-0, Nice, France, 22-27 Aug. 2010
- Mitrokotsa A., Rieback M. R. & Tanenbaum A. S. (2008). Classification of RFID Attacks, IWRT, June 2008
- MobileCloak, The off switch for "always on" mobile wireless devices, spy chips, toll tags, RFID tags and technologies, 17.02.11, Available from: www.mobilecloak.com
- Oren Y. and Wool A. (2009). Relay Attacks on RFID-Based Electronic Voting Systems, IACR ePrint, August 2009
- Reinhold P. (1993) Elektrotechnik 1-Felder und einfache Stromkreise, 3rd edn, Springer-Verlag, Berlin/Heidelberg, ISBN 3-540-55753-9, 1993
- RFIDzapper . 17.02.11, Available from: <https://wiki.c3le.de/wiki/RFID-Zapper>
- RFIDzapper(EN) (2006). RFID-Zapper(EN), 17.02.11, Available from: http://events.ccc.de/congress/2005/static/r/f/i/RFID-Zapper%28EN%29_77f3.html
- HF Antenna Cookbook. Texas Instruments, 17.02.11, Available from: <http://www.ti.com/rfid/docs/manuals/appNotes/HFAntennaCookbook.pdf>
- Tobergte W. & Bienert R. (2007). Eavesdropping and activation distance for ISO/IEC 14443 devices, NXP White Paper, 2007
- Verdult R. (2008). Security analysis of RFID tags, Master Thesis, Information Security Group (GSI), Belgium
- Youbok L. (1999). Antenna circuit design, AN710, application note, microID 13.56MHz – RFID system design guide, Microchip, 17.02.11, Available from: <http://www.microchip.com>

Zetter K. (2006). Hackers Clone E-Passports, 17.02.11, Available from:
[http://www.wired.com/science/discoveries/news/2006/08/71521?currentPage=](http://www.wired.com/science/discoveries/news/2006/08/71521?currentPage=1)
1

IntechOpen

IntechOpen



Current Trends and Challenges in RFID

Edited by Prof. Cornel Turcu

ISBN 978-953-307-356-9

Hard cover, 502 pages

Publisher InTech

Published online 20, July, 2011

Published in print edition July, 2011

With the increased adoption of RFID (Radio Frequency Identification) across multiple industries, new research opportunities have arisen among many academic and engineering communities who are currently interested in maximizing the practice potential of this technology and in minimizing all its potential risks. Aiming at providing an outstanding survey of recent advances in RFID technology, this book brings together interesting research results and innovative ideas from scholars and researchers worldwide. Current Trends and Challenges in RFID offers important insights into: RF/RFID Background, RFID Tag/Antennas, RFID Readers, RFID Protocols and Algorithms, RFID Applications and Solutions. Comprehensive enough, the present book is invaluable to engineers, scholars, graduate students, industrial and technology insiders, as well as engineering and technology aficionados.

How to reference

In order to correctly reference this scholarly work, feel free to copy and paste the following:

Pierre-Henri Thevenon, Olivier Savry, Smail Tedjini and Ricardo Malherbi-Martins (2011). Attacks on the HF Physical Layer of Contactless and RFID Systems, Current Trends and Challenges in RFID, Prof. Cornel Turcu (Ed.), ISBN: 978-953-307-356-9, InTech, Available from: <http://www.intechopen.com/books/current-trends-and-challenges-in-rfid/attacks-on-the-hf-physical-layer-of-contactless-and-rfid-systems>

INTECH
open science | open minds

InTech Europe

University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China

Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821

© 2011 The Author(s). Licensee IntechOpen. This chapter is distributed under the terms of the [Creative Commons Attribution-NonCommercial-ShareAlike-3.0 License](https://creativecommons.org/licenses/by-nc-sa/3.0/), which permits use, distribution and reproduction for non-commercial purposes, provided the original is properly cited and derivative works building on this content are distributed under the same license.

IntechOpen

IntechOpen